Empty or void relation. If A is a set, then every subset of $A \times A$ is a relation on A. Since the null set ϕ is the subset of all the sets and so is of the set $A \times A$, therefore ϕ is also a relation on A. Such a relation is said to be the Empty or Void relation on A:

Inverse relation. If R be a relation from a set A to another set B, then the inverse relation of R denoted by R^{-1} is defined as the inverse relation, *i.e.*, R^{-1} from B to A iff

$$R^{-1} = \{(y, x)\} : \{(x, y) \in R\}$$

clearly
$$\text{Dom}\,(R^{-1}) = \text{Ran}\,(R)$$
$$\text{Ran}\,(R^{-1}) = \text{Dom}\,(R)$$

so that
$${}_xR_y \Leftrightarrow {}_yR_x^{-1}$$

If $A = B$, R and R^{-1} both are the relations on A.

It is easy to verify that $(R^{-1})^{-1} = R$.

Types of Relations

I. **Reflexive.** A relation R on a set A is reflexive iff each member of A is R-related to itself, *i.e.*, ${}_xR_x \ \forall\ x \in A$ or in other words, $(x, x) \in R \ \forall\ x \in A$. Evidently a relation R on A is reflexive iff $\Delta_A \subset R$, Δ_A being identity relation, *e.g.*, if A be the set of lines in a plane and R a relation 'parallel to' then any line $x \in A$ is parallel to itself, *i.e.*, ${}_xR_x \ \forall\ x \in A$ and so R is reflexive.

II. **Symmetric.** A relation R on a set A is symmetric iff ${}_xR_y \Rightarrow {}_yR_x$; $x, y \in A$

i.e., $(x, y) \in R \Rightarrow (y, x) \in R$

Evidently a relation R on A is symmetric iff $R^{-1} = R$.

e.g., ${}_xR_y$ = '$(x - y)$ is even number' is symmetric since $y - x$ is also even, when $(x - y)$ is even.

III. **Transitive.** A relation R on a set A is transitive iff

$${}_xR_y \text{ and } {}_yR_x \Rightarrow {}_xR_z;\ x, y, z \in A$$

i.e., $(x, y) \in R$ and $(y, z) \in R \Rightarrow (x, z) \in R$

Evidently a relation R on A is transitive iff $RoR \subset R$

e.g., the relation $x < y$ is transitive since if $x < y$ and $y < z$ then $x < z$.

IV. **Anti-symmetric.** A relation R on a set A is anti-symmetric iff we never have ${}_xR_y$ and ${}_yR_x$ both: $x, y \in A$ except when $x = y$

i.e.,
$${}_xR_y \text{ and } {}_yR_x \Rightarrow x = y;\ x, y \in A$$

or $(x, y) \in R$ and $(y, x) \in R \Rightarrow x = y$; $x, y \in A$

Evidently a relation R on A is anti-symmetric iff $R \cap R^{-1} \subset \Delta_A$, Δ_A being identity relation or in other words, $R \cap R^{-1} = \phi$.

e.g., ${}_xR_y$ = 'x, divides y' in $\mathbf{Z}$ (set of natural numbers) is anti-symmetric since 'x divides y' and 'y divides x' $\Rightarrow x = y$; $x, y \in \mathbf{Z}$

i.e., ${}_xR_y$ and ${}_yR_x \Rightarrow x = y$; $x, y \in \mathbf{Z}$

Equivalence relation. A relation R over a set S is said to be an equivalence relation if it satisfies the following properties:

(*i*) *Reflexivity, i.e.*, $\forall\ x \in S$, ${}_xR_x$ or $x \sim x \ \forall\ x$ ($\sim$ called *wiggle*)

(*ii*) *Symmetry, i.e.*, ${}_xR_y \Rightarrow {}_yR_x$ or $x \sim y \Rightarrow y \sim x$

(*iii*) *Tansitivity, i.e.*, ${}_xR_y$ and ${}_yR_x \Rightarrow {}_xR_z$ or $x \sim y$ and $y \sim z \Rightarrow x \sim z$.

Equivalence set (or class). Let R be an equivalence relation in a non-empty set S and let x be an element of S, *i.e.*, $x \in S$; then the elements $y \in S$ satisfying ${}_yR_x$ constitute a subset of S, known as equivalence set of x w.r.t. R, *i.e.*,

$$S_x \text{ or } \bar{x} \text{ or } [x] = \{y\,;\, y \in S \text{ and } {}_yR_x\}$$

The equivalence set has the following properties:

(*i*) If $z \in [x]$ then $[z] = [x]$

(*ii*) $[x] = [z]$ iff ${}_xR_z$

(*iii*) If $[x] \cap [z] \neq \phi$, then $[x] = [z]$

Partition set. Given a non-empty set S a set $P = \{X, Y, Z....\}$ of non-empty subsets of S is called a partition of S, provided

(*i*) $X \cup Y \cup Z \cup ... = S$

(*ii*) The intersection of every pair of distinct subsets of $S \in \mathbf{P}$ is the null set, *e.g.*, if $X, Y \in \mathbf{P}$ then either $X = Y$ or $X \cap Y = \phi$.

e.g., if $S = \{1, 2, 3, 4, 5\}$ then $\{1, 3, 5\}$, $\{2, 4\}$, and $\{1, 2, 3\}$, $\{4, 5\}$ are two different partitions of S.

Quotient set. If R be an equivalence relation defined on a non-empty set S, then the set of mutually exclusive sets in which S is partitioned w.r.t. the equivalence relation R, is called as quotient set of S for the equivalence relation R and is denoted by $\bar{S}$ or S/R.

e.g., the set $\mathbf{I}$ of all integers for the equivalence relation modulo 5 is the set $\mathbf{I}/R = \{[0], [1], [2], [3]\ [4]\}$.

Note. Two integers p an q are said to be *congruent modulo m* denoted by $p \equiv q \pmod{m}$ if $p - q$ is exactly divisible by m, *i.e.*, $(p - q)$ is an integral multiple of m.

A note on binary operations. A binary operation (or simply composition) usually denoted by o (or sometimes by $\cdot$, *, $\oplus$ etc.) is used to combine two elements of a set in order to produce another element of the set. In other words, a binary operation in a set S is a function $f: S \times S \to S$., *e.g.*, the binary operation 'addition' on any two elements of $\mathbf{I}$ (set of integers) gives another integer belonging to $\mathbf{I}$.

(*i*) Such an operation is *commutative* if $xoy = yox\ \forall\ x, y \in S$

(*ii*) It is *associative* if $xo\,(yoz) = (xoy)\,oz\ \forall\ x, y, z \in S$

(*iii*) It is *distributive* w.r.t. another binary operation $\oplus$ if

$$xo\,(y \oplus z) = (xoy) \oplus (xoz) \text{ (left distributive)}$$

and

$$(y \oplus z)\,ox = (yox) \oplus (zox) \text{ (right distributive)}\ \forall\ x, y, z \in S.$$

(*iv*) It is said to have *identity element* if $\exists\ e \in S$ s.t. $xoe = eox$

$$= x\ \forall\ x \in S$$

(*v*) It is *invertible* if corresponding to an $x \in S\ \exists$ a $y \in S$ s.t.

$$xoy = e = yox$$

i.e., y is the inverse of x w.r.t. 'o' and vice versa.

(*vi*) It satisfies *concellation law* if $\forall\ x, y, z \in S$

$$xoy = xoz \Rightarrow y = z \quad \text{(left cancellation law)}$$

$$yox = zox \Rightarrow y = z \quad \text{(right cancellation law)}$$

e.g., consider two binary operations o and $\cdot$ defined on $\mathbf{I}$ (set of all integers) such that

$$xoy = x + 2y \quad \text{and} \quad x \cdot y = 2xy\ \forall\ x, y \in \mathbf{I}.$$

(v) Since 'o' has no identity element, it is not invertible.
Assuming that '$\cdot$' has an inverse p, we must have

$$x \cdot p = e = p \cdot x \quad \forall\ x \in \mathbf{I}$$

Now $\quad x \cdot p = e \Rightarrow 2xp = e = \frac{1}{2}$

$$\Rightarrow p = \frac{1}{4x}$$

and $\quad p \cdot x = e \Rightarrow 2px = \frac{1}{2} \Rightarrow p = \frac{1}{4x}$

Hence '$\cdot$' is invertible and inverse of x is $\frac{1}{4x}$.

(vi) We have $xoy = x + 2y$ and $xoz = x + 2z \quad \forall\ x, y, z \in \mathbf{I}$
so that $xoy = xoz \Rightarrow x + 2y = x + 2z \Rightarrow y = z$, *i.e.*, left cancelllation law holds for 'o'
and $\quad x \cdot y = 2xy,\ x \cdot z = 2xz \quad \forall\ x, y, z \in \mathbf{I}$
so that $\quad x \cdot y = x \cdot z \Rightarrow 2xy = 2xz \Rightarrow y = z$, *i.e.*, left cancellation law holds for '$\cdot$'
Also $\quad yox = y + 2x$ and $zox = z + 2x \quad \forall\ x, y, z \in \mathbf{I}$
So $\quad yox = zox \Rightarrow y + 2x = z + 2x \Rightarrow y = z$, *i.e.*, right cancellation law holds for 'o'.
and $\quad y \cdot x = 2yz,\ z \cdot x = 2zx \quad \forall\ x, y, z \in \mathbf{I}$
So $\quad y \cdot x = z \cdot x \Rightarrow 2yz = 2zx$
$\Rightarrow y = z$, *i.e.*, right cancellation law holds for '$\cdot$'

Hence cancellation law holds for o and $\cdot$ both the binary operations.

4.2 GROUPS

A group is the simplest algebraic structure found in nature wherever symmetry exists.

A group (G, o) is a system consisting of a non-empty set G such as $G = \{a, b, c, ...\}$ and a binary operation 'o' satisfying the following axioms:

G_1—(*Closure*). If $a \in G$, $b \in G$ then $aob \in G$ or in other words if $a \in G$, $b \in G$ then $aob = c$ (closure) where $c \in G$.

G_2—(*Associativity*). If $a, b, c \in G$ then $ao\,(boc) = (aob)oc$.

G_3—(*Existence of an identity*). If $a \in G$, then $\exists$ an identity element $e \in G$ s.t. $eoa = a$ $\forall\ a \in G$

G_4—(*Existence of an inverse*). If $a \in G$, $\exists$ an inverse $a^{-1} \in G$ s.t. $a^{-1}\,oa = e$ where $e \in G$, being an identity element.

In addition to these four axioms if a fifth axiom of commutativity namely G_5 is also satisfied, *i.e.*,

G_5—(*Commutation*). If $a, b \in G$ the $aob = boa$ so that G_3 and G_4 take the forms

$$G_3: eoa = aoe = a$$

$$G_4: aoa^{-1} = a^{-1}oa = e$$

then the group is said to be an *Abelian group*.

e.g., the set $\mathbf{I}$ (of all integers) with the binary operation 'o' taken as additive (+) is a group, for it satisfies all the four axioms

G_1—if $a, b \in \mathbf{I}$, then $a + b \in \mathbf{I}$

G_2— if $a, b, c, \in \mathbf{I}$, then $a + (b + c) = (a + b) + c$

G_3—if $a \in \mathbf{I}$ then $\exists$ an integer zero (0) such that $0 + a = a$

G_4— if $a \in \mathbf{I}$, then $\exists$ an inverse $(-a)$ s.t. $-a + a = 0$ (identity element).

This group is also abelian or commutative as G_5 is also satisfied, *i.e.*, $G_5 - a, b \in \mathbf{I}$, $a + b = b + a$.

Finite and Infinite groups. A group (G, o) consisting of a finite number of elements is said to be a *finite group*, e.g., the set $S = \{1, \omega, \omega^2\}$ where $\omega^3 = 1$, is a finite group under multiplication composition.

A group (G, o) consisting of an infinite number of elements is said to be an *infinite group*, e.g., the set $\mathbf{I}$ (of all integers) is an infinite group under the addition composition.

Order of a group. The number of elements in a finite group is known as the order of the group. The infinite set is said to be of infinite order. As an example the set $\{1, -1\}$ under multiplication composition is a group of order 2.

4.3 ELEMENTARY PROPERTIES OF A GROUP

I. **Uniqueness of identity**, *i.e., the identity element of a group* (G, o) *is unique.*

If possible let us assume that e and e' are two identity elements of the group (G, o), then

$$eoa = aoe = a \ \forall \ a \in G \quad \text{... (1)}$$

and

$$e'oa = aoe' = a \ \forall \ a \in G \quad \text{... (2)}$$

Putting $a = e'$ in (1), we have

$$eoe' = e'oe = e' \quad \text{... (3)}$$

Also putting $a = e$ in (2), we have

$$e'oe = eoe' = e \quad \text{... (4)}$$

From (3) and (4) it follows that $e' = e$, *i.e.*, there cannot be two identity elements for (G, o) and hence the identity element of a group is unique.

II. **Uniqueness of Inverse**, *i.e., in a group* (G, o) *every element possesses a unique inverse.*

If possible let us assume that a' and a^{-1} are two inverses of a. Also let $a \in G$ and e be the identity element of G. Then we have

$$a^{-1}oa = aoa^{-1} = e \quad \text{... (1)}$$

$$a'oa = aoa' = e \quad \text{... (2)}$$

Post-multiplying (1) by a' we get

$$(a^{-1}oa)oa' = (aoa^{-1})oa' = eoa' = a' \quad \text{... (3)}$$

and premultiplying (2) by a^{-1} we get

$$a^{-1}o(a'oa) = a^{-1}o(aoa') = a^{-1}oe = a^{-1} \quad \text{... (4)}$$

But group-postulate G_2 gives

$$(a^{-1}oa)oa' = a^{-1}o(aoa')$$

$\therefore$ (3) and (4) follow that $a' = a^{-1}$, *i.e.*, the inverse of an element in a group is unique.

Aliter. Taking a^{-1} and a' two inverses of $a \in G$, we have

$$aoa' = a'oa = e \text{ and } a^{-1}oa = aoa^{-1} = e$$

$$\therefore \quad a^{-1} = a^{-1}oe = a^{-1}o(aoa') = (a^{-1}oa)oa' = eoa' = a'$$

which follows the uniqueness of inverse of $a \in G$.

III. **Cancellation laws**, *i.e., for any group* (G, o), *and* $a, b, c \in G$, *the following laws hold*

(*i*) $aob = aoc \Rightarrow b = c$ (*left cancellation law*)

(*ii*) $boa = coa \Rightarrow b = c$ (*right cancellation law*)

G_3—if $a \in \mathbf{I}$ then $\exists$ an integer zero (0) such that $0 + a = a$

G_4— if $a \in \mathbf{I}$, then $\exists$ an inverse $(-a)$ s.t. $-a + a = 0$ (identity element).

This group is also abelian or commutative as G_5 is also satisfied, *i.e.*, G_5 — a, b $a + b = b + a$.

Finite and Infinite groups. A group (G, o) consisting of a finite number of elem is said to be a *finite group*, e.g., the set $S = \{1, \omega, \omega^2\}$ where $\omega^3 = 1$, is a finite group un multiplication composition.

A group (G, o) consisting of an infinite number of elements is said to be an *infi group*, e.g., the set $\mathbf{I}$ (of all integers) is an infinite group under the addition composition

Order of a group. The number of elements in a finite group is known as the order the group. The infinite set is said to be of infinite order. As an example the set $\{1,$ under multiplication composition is a group of order 2.

4.3 ELEMENTARY PROPERTIES OF A GROUP

I. **Uniqueness of identity,** *i.e., the identity element of a group* (G, o) *is unique.*

If possible let us assume that e and e' are two identity elements of the group (G, o), then

$$eoa = aoe = a \ \forall \ a \in G \quad \ldots(1)$$

and

$$e'oa = aoe' = a \ \forall \ a \in G \quad \ldots(2)$$

Putting $a = e'$ in (1), we have

$$eoe' = e'oe = e' \quad \ldots(3)$$

Also putting $a = e$ in (2), we have

$$e'oe = eoe' = e \quad \ldots(4)$$

From (3) and (4) it follows that $e' = e$, *i.e.*, there cannot be two identity elements (G, o) and hence the identity element of a group is unique.

II. **Uniqueness of Inverse,** *i.e., in a group* (G, o) *every element possesses a uniq inverse.*

If possible let us assume that a' and a^{-1} are two inverses of a. Also let $a \in G$ and e the identity element of G. Then we have

$$a^{-1}oa = aoa^{-1} = e \quad \ldots(1)$$

$$a'oa = aoa' = e \quad \ldots(2)$$

Post-multiplying (1) by a' we get

$$(a^{-1}oa)oa' = (aoa^{-1})oa' = eoa' = a' \quad \ldots(3)$$

and premultiplying (2) by a^{-1} we get

$$a^{-1}o(a'oa) = a^{-1}o(aoa') = a^{-1}oe = a^{-1} \quad \ldots(4)$$

But group-postulate G_2 gives

$$(a^{-1}oa)oa' = a^{-1}o(aoa')$$

$\therefore$ (3) and (4) follow that $a' = a^{-1}$, *i.e.*, the inverse of an element in a group is unique.

Aliter. Taking a^{-1} and a' two inverses of $a \in G$, we have

$$aoa' = a'oa = e \text{ and } a^{-1}oa = aoa^{-1} = e$$

$$\therefore \quad a^{-1} = a^{-1}oe = a^{-1}o(aoa') = (a^{-1}oa)oa' = eoa' = a'$$

which follows the uniqueness of inverse of $a \in G$.

III. **Cancellation laws,** *i.e., for any group* (G, o), *and* $a, b, c \in G$, *the following laws hold*

(*i*) $aob = aoc \Rightarrow b = c$ (*left cancellation law*)

(*ii*) $boa = coa \Rightarrow b = c$ (*right cancellation law*)

(*i*) Taking $a^{-1} \in G$ as the inverse of $a \in G$, we have

$aob = aoc \Rightarrow a^{-1}o(aob) = a^{-1}o(aoc)$ on premultiplying by a^{-1}

$\Rightarrow (a^{-1}oa)ob = (a^{-1}oa)oc$, the composition being associative by G_2

$\Rightarrow eob = eoc$, since $\exists$ an identity element $e \in G$ for 'o'

$\Rightarrow b = c$.

(*ii*) Again taking $a^{-1} \in G$ as the inverse of $a \in G$, we have

$boa = coa \Rightarrow (boa)oa^{-1} = (coa)oa^{-1}$ on postmultiplying by a^{-1}

$\Rightarrow bo(aoa^{-1}) = co(aoa^{-1})$ by G_2

$\Rightarrow boe = coe \quad \because \exists$ an identity element $e \in G$ for 'o'

$\Rightarrow b = c$.

Note. $aoc = cob \Rightarrow a = b$ unless the group is abelian.

IV. Uniqueness of solutions, *i.e., if $a, b \in G$, then the equations $aox = b$ and $yoa = b$ have unique solutions in G.*

If a^{-1} be the inverse of $a \in G$, then $a^{-1} \in G$ and $aoa^{-1} = e$ (identity element).

Now $a^{-1} \in G$ and $b \in G \Rightarrow a^{-1}\, ob \in G$

Putting $x = a^{-1}ob$ in the equaiton $aox = b$, we get

$$ao(a^{-1}ob) = b$$

or $\quad (aoa^{-1})ob = b$ by G_2

or $\quad eob = b$, *i.e.*, $b = b$

which follows that $x = a^{-1}ob$ is a solution of $aox = b$.

To show that this solution is unique, let us assume that y is an element different from $a^{-1}ob$ in G s.t. it satisfies the equation $aox = b$. Then,

$$aoy = b = eob = (aoa^{-1})ob = ao(a^{-1}ob) \text{ by } G_2.$$

so that left cancellation law yields $y = a^{-1}ob$.

As such $x = y$, *i.e.*, the solution is unique.

Again, $b \in G$ and $a^{-1} \in G \Rightarrow boa^{-1} \in G$

Putting $y = boa^{-1}$ in $yoa = b$, we get

$(boa^{-1})oa = b$ or $bo(a^{-1}\, oa) = b$ by G_2

or $\quad boe = b$, *i.e.*, $b = b$

which follows that $y = boa^{-1}$ is a solution of $yoa = b$.

To show that this solution is unique, let us assume that z is an element different from boa^{-1} in G s.t. it satisfies the equation $yoa = b$.

Then $\quad zoa = b = boe = bo\,(a^{-1}oa) = (boa^{-1})\, oa$ by G_2.

The right cancellation law gives $z = boa^{-1}$

so that $y = z$ and hence the solution is unique.

Note. The unique solution of $xox = x$ is $x = e$ in group (G, o)

V. Inverse of the inverse is itself, *i.e., if $a \in G$ then $(a^{-1})^{-1} = a$.*

Inverse law gives $(a^{-1})^{-1}oa^{-1} = e$, e being identity element in G.

Postmultiplying by a, we get

$$[(a^{-1})^{-1}oa^{-1}]oa = eoa$$

or $\quad (a^{-1})^{-1}o(a^{-1}oa) = a$ by G_2

or $\quad (a^{-1})^{-1}oe = a$ by G_4

or $\quad (a^{-1})^{-1} = a$ by G_3

which proves the proposition.

sub-group of G, if the binary operation 'o' in G induces a binary operation in H and the elements of H obey the group axioms.

In other words, a non-empty subset H of a group G is said to be a sub-group of G if it satisfies the following two axioms:

(i) $a, b \in H \Rightarrow aob \in H$,

(ii) $a \in H \Rightarrow a^{-1} \in H$

e.g., the set of even integers is a sub-group of the additive group of integers.

Proper sub-group. A sub-group of a group (G, o) other than G itself and the group consisting of the identity element alone is termed as a proper sub-group of G. *e.g.*, the additive group of integers is a proper sub-group of the additive group of rational numbers.

Improper or trival sub-groups. The group (G, o) itself and the group consisting of identity alone, *i.e.*, $(\{e\}, o)$ are known as trivial or improper sub-groups of (G, o).

Order of an element of a group. Let a be an element of a group (G, o), *i.e.*, $a \in G$. Then the order of a is the least positive integer n s.t. $a^n = e$.

In case $\nexists$ such integer, the order of a is said to be zero or infinite. *e.g.*, the order of the element -1 in the multiplicative group $\{1, -1, i, -i\}$ is 2 since $(-1)^2 = 1$, the identity element. The order of i is 4 since $i^4 = 1$.

Addition modulo m, (m being an integer). If a and b are two integers and m a positive integer, then 'addition modulo m' is denoted by $a +_m b$ and defined as $a +_m b = r$, $o \le r < m$ where r is the least positive remainder obtained on dividing the sum of a and b by m.

e.g. $12 +_3 5 = 2$ since $12 + 5 = 3(5) + 2$

and $-5 +_4 10 = 1$ since $-5 + 10 = 4(1) + 1$

Multiplication modulo p, (p being a prime). If a and b are two integers and p, a positive integer, then 'multiplication modulo p', is denoted by $a \times_p b$ and defined as $a \times_p b = r$, $o \le r < p$ where r is the remainder obtained on dividing the ordinary product ab by p.

e.g., $9 \times_6 7 = 3$ since $9 \times 7 = (6)\ 10 + 3$

and $-7 \times_5 8 = 4$ since $-7 \times 8 = (5)\ (-12) + 4$

Group table or Composition table. It is commonly observed that a 'table' is a convenient way of either defining a binary operation in a finite set S or tabulating the effect of a binary operation in a set S. In forming a table or say a group table we arrange the elements of a group in rows and columns of a square array such that each element of the group occurs once and only once in each row or column. The composition element aob occurs at the intersection of row and column of the elements a and b of the group after the binary operation has been performed. For example consider a set

$S = \{1, 2, 3\}$ and let '$\cdot$' be the binary operation in S defined by

$\therefore$ $(1, 1) \to 1$, $(1, 2) \to 2$, $(1, 3) \to 3$, $(2, 1) \to 2$, $(2, 2) \to 1$, $(2, 3) \to 2$,
$(3, 1) \to 3$, $(3, 2) \to 2$, $(3, 3) \to 1$

then these operations can be arranged in a table as follows:

$\cdot$	1	2	3
1	1	2	3
2	2	1	2
3	3	2	1

It is clear that (i, j)th square $(i, j = 1, 2, 3)$ is the intersection of ith row (*i.e.*, row labelled or faced by i) and jth column (*i.e.*, column labelled or faced by j) and in this square we have put the element obtained by the binary operation '$\cdot$' on (i, j) such as, $\therefore (1, 2) \to 2$

V1. Reversal law, *i.e.*, if $a, b \in G$ *then* $(aob)^{-1} = b^{-1} oa^{-1}$.

Let e be the identity element in G.

Now $a \in G \Rightarrow a^{-1} \in G$ and $b \in G \Rightarrow b^{-1} \in G$

$$\begin{aligned} \therefore \quad (b^{-1}oa^{-1})o(aob) &= b^{-1}o[a^{-1}o(aob)] \text{ by } G_2 \\ &= b^{-1}o[(a^{-1}oa)ob] \text{ by } G_2 \\ &= b^{-1}o[eob] \text{ by } G_4 \\ &= b^{-1}ob \text{ by } G_3 \\ &= e. \end{aligned}$$

Hence by definition of inverse element of a group $b^{-1}oa^{-1}$ is the inverse of a

$$(aob)^{-1} = b^{-1}oa^{-1}.$$

Note. The result may be generalized for any number of elements $a_1, a_2, a_3, \ldots\ldots a_n \in G$, where we have

$$(a_1oa_2o\ldots\ldots oa_n)^{-1} = a_n^{-1}oa_{n-1}^{-1}o\ldots\ldots oa_2^{-1}oa_1^{-1}.$$

4.4 SOME DEFINITIONS

Semi-group. A set S with a binary operation 'o' is said to be a semi-group if it sa the following two axioms:

S_{G1}—(*Closure*). $a \in S, b \in S \Rightarrow aob \in S$.

S_{G2}—(*Associativity*). If $a, b, c \in S$ then $(aob)\,oc = ao\,(boc)$.

Theorem. *A semi-group* (G, o) *satisfying the following postulates is a group:*

(1) *G has a left identity e s.t.* $eoa = a \;\forall\; a \in G$.

(2) *Every element a in G has a left inverse* a^{-1} *in G s.t.* $a^{-1}oa = e$.

Since (G, o) is a semi-group, therefore by definition it follows that

(*i*) (G, o) satisfies the closure law.

(*ii*) (G, o) satisfies the associative law.

(*iii*) a^{-1} being the left inverse of a and e the left identity we have

$$\begin{aligned} a^{-1}o(aoe) &= (a^{-1}oa)oe && \text{by } (ii) \\ &= eoe && \text{by postulate (2)} \\ &= e && \text{by postulate (1)} \\ &= a^{-1}oa && \text{by postulate (2)} \end{aligned}$$

So that by left cancellation law, $aoe = a$

which follows that e is also a right identity.

Hence the identity element exists for the composition.

(*iv*) We have $a^{-1}o(aoa^{-1}) = (a^{-1}oa)oa^{-1}$ by (*ii*)

or

$$\begin{aligned} a^{-1}o(aoa^{-1}) &= eoa^{-1} \text{ by (2)} \\ &= a^{-1} \text{ by (1)} \\ &= a^{-1}oe, \text{ since identity element exists for '}o\text{'}, \end{aligned}$$

$$\therefore \quad aoa^{-1} = e \text{ by left cancellation law.}$$

which shows that a^{-1} is also a right inverse of a.

Hence every element of G has an inverse.

Since all the four group axioms are satisfied, therefore a semi-group with the given postulates is a group.

Sub-group. *A sub-group of a group* (G, o) *is any collection of elements of G satisfy the axioms of G. In other words, a non-empty subset say H of a group G is said to be*

► **Example 17.5** *Check the following multiplication table for the set of fourth roots of unity, namely* $\{1, -1, i, -i\}$ *for its group properties.*

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(Burdwan and Calcutta Hons.)

Solution. The table shows that

(i) the *closure property* holds good,

(ii) the operation is *associative*,

(iii) the set has 1 as *identity element* in respect of the given operation, and

(iv) each element has an *inverse*.

Hence the set forms a multiplicative group as all the group conditions are satisfied. Further, the set is *commutative* with respect to multiplication. So, it forms an ***abelian group.***

● If the composition table with the corresponding operation possesses a symmetry across its main diagonal, the group is *commutative.*

► **Example 17.6** *Show that the following four* 2×2 *matrices constitute a multiplicative group :*

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \; C = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}, \; D = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}$$

Solution. We note that A is a unit matrix. So, we have

$$AA = A, \;\; AB = BA = B, ; \; AC = CA = C, \;\; AD = DA = D$$

Also, $$BC = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = D; \quad BD = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = C$$

Similarly, $CB = D$, $DB = C$. Also, $BB = CC = DD = A$ and $CD = DC = B$.

Hence, the composition table is as given under.

$\times$	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

► **Example 17.7** *Show that the set* $S = \{1, \omega, \omega^2\}$, *where* ω *is a cube root of unity forms a finite abelian group under the composition of multiplication.* **(Burdwan Hons.)**

Solution. We have the set $S = \{1, \omega, \omega^2\}$ where $\omega^3 = 1$.

The composition table under multiplication is shown as under.

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$\because\ \omega^3 = 1;\ \omega^4 = \omega^3 \cdot \omega = \omega$

All the elements in group table belong to S so that the *closure* axiom is satisfied. Multiplication of complex numbers is associative. So, the *associativity* condition is also satisfied. Plainly, the *identity* element $1 \in S$, and the third axiom is satisfied. The *inverses* of $1, \omega, \omega^2$ are respectively $1, \omega^2, \omega \in S$ and the fourth axiom is satisfied.

The *commutative* property is also satisfied as $1 \cdot \omega = \omega \cdot 1 = \omega$ etc.

Further, the set has a *finite* number of elements and thus forms a ***finite abelian group*** under multiplication.

▶ **Example 17.8** *Show that the set of all nth roots of unity form a finite abelian group G of order n under multiplication.* **(Burdwan Hons.)**

Solution. The nth roots of unity by De Moivre's theorem are

$$(1)^{1/n} = (\cos 2r\pi + i \sin 2r\pi)^{1/n} = \cos 2r\pi/n + i \sin 2r\pi/n, \quad r = 0, 1, 2, \cdots, n-1$$

Thus the nth roots of unity are

$$1,\ \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},\ \cos 2\frac{2\pi}{n} + i\sin 2\frac{2\pi}{n}, \cdots, \cos\frac{(n-1)2\pi}{n} + i\sin\frac{(n-1)2\pi}{n}$$

or, $1,\ e^{1\cdot 2\pi i/n},\ e^{2\cdot 2\pi i/n}, \cdots, e^{(n-1)2\pi i/n}$.

Now, the multiplication of complex number is *associative.*

There is an *identity element,* $e^{2\pi i \cdot 0/n} = 1$.

Since $e^{2\pi i r/n} \cdot e^{2\pi i(n-r)/n} = e^{2\pi i n/n} = e^{2\pi i} = 1$, the *inverse* of $e^{2\pi i r/n}$ is $e^{2\pi i(n-r)/n}$.

We shall now show that the product of any two elements in the set is the element of the set. If $a = e^{p\cdot 2\pi i/n}$, $b = e^{q\cdot 2\pi i/n} \in G$ where $0 \le p \le n-1$, $0 \le q \le n-1$, then $ab = e^{(p+q)2\pi i/n}$ will belong to G if $p+q \le n-1$. Assume $p+q > n-1 \Rightarrow p+q = n+m$ where $m \le n-2$, since the maximum value of $p+q$ can be $2(n-1)$, that is, $2n-2$.

$$\therefore\ ab = e^{(n+m)2\pi i/n} = e^{2\pi i} \cdot e^{2\pi i m/n} = e^{2\pi i m/n},$$

since $e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1$.

So, all the conditions of G for being a group are satisfied.

Further, since the multiplication of complex numbers is *commutative* and the number of elements n is ***finite***, G is a ***finite abelian group.***